United States Department of Agriculture

Office of the Chief Information Officer

1400 Independence Avenue S.W.

Washington, DC 20250

MAR 9 2006

TO: All Employees and Contractors
Office of the Chief Information Officer

FROM: David M. Combs
Chief Information Officer

SUBJECT: OCIO Security Agreement

USDA Departmental Memorandum 3545-001, *Computer Security Training And Awareness Chapter 9, Part 1,* requires periodic training in computer security awareness and accepted computer security practices. It also requires that all agency employees sign a computer user security agreement that lists key computer security policies and objectives.

To accomplish this, the OCIO is implementing an OCIO Security Agreement, which is attached. Our goal is to have a signed OCIO Security Agreement in place for each worker (both government workers and contractors). This security agreement will help the OCIO ensure that all workers involved in the management, use, design, development, maintenance or operation of an automated information system are aware of their security responsibilities and are trained to those responsibilities.

Supervisors and Contracting Officer Technical Representatives (COTR) will obtain a signed OCIO Security Agreement from each worker by 30 April 2006. It is expected that each supervisor and/or COTR will retain the original agreement and that a copy will be given to the employee/contract worker.

Attachment: OCIO Security Agreement

OCIO Security Agreement

An agreement between _____ and the USDA Office of the Chief Information Officer (OCIO).
(Name -- Printed or Typed)

1. PURPOSE. This document is meant to obtain an individual agreement to abide by security requirements and procedures needed to protect OCIO and customer information resources. It is also intended to help raise security awareness and inform workers about security policies and procedures and to provide workers an opportunity for asking questions about these matters.

2. AUTHORITIES. National policy requirements regarding information systems are stated in the Federal Information Security Management Act (Title III of the E-Government Act of 2002); the Computer Fraud and Abuse Act (18 U.S.C. Sec. 1030 [1993]); Office of Management and Budget (OMB) Circular No. A-123, Management Accountability and Control; and OMB Circular A-130, Management of Federal Information Resources. These documents along with USDA security policies, prescribe and set standards for establishing and maintaining a comprehensive information security program and use of information systems.

3. SCOPE. This agreement applies to OCIO workers (both employees and contractors) who operate, maintain, and/or use OCIO Information Technology (IT) systems.

4. UNDERSTANDING AND AGREEMENTS. As a user of OCIO IT systems, I:

- **Will protect OCIO and customer systems in accordance with Federal, USDA, and OCIO policies.**
- **Will use USDA and/or OCIO computer systems (e.g., computers, systems, laptops, PEDs, networks, etc.) only for authorized purposes. If using the computer systems and networks for nonofficial purposes, I will do so within the bounds allowed by USDA policy, supervisor approval, and without interfering with official business.**
- **Will protect systems and all sensitive information from electronic or physical access by unauthorized personnel. I will protect computer equipment, media, telecommunications, and similar assets from theft, fraud, misuse, loss, unauthorized modification, and unauthorized denial of use. I will make every effort to avoid action/inaction that could jeopardize mission success, customer rights, individual privacy, or the reputation of the OCIO.**
- **Understand that systems and other information resources, including electronic mail and Internet access, are primarily intended for official business and may be monitored. Although USDA policy permits limited personal use, I understand that my personal use must not interfere with official business and that I have no expectation of personal privacy when using these systems.**
- **Will not intentionally access, delete or alter files, operating systems or programs, except as specifically authorized for official business.**
- **Will not leave OCIO computers in an operational state (e.g., "logged on") while unattended. I will either turn off the computer system, manually lock the screen, or set a time activated password-protected screen saver.**
- **Will abide by software copyright licenses and restrictions. I will not load any unapproved software (e.g., software from home, games, etc.) or install hardware or peripheral devices (e.g., external hard drives, docking stations, thumb drives, etc) on OCIO systems without my supervisor's permission.**
- **Will not download file-sharing software (e.g., MP3 music, video files, etc.), peer-to-peer software (e.g., Kazaa, Napster, etc.), or games onto OCIO systems or networks.**

_____
(Initials)

OCIO Security Agreement

- **Acknowledge that I will receive user identifiers (user IDs) and passwords to authenticate my computer account. After receiving them, I will:**
  - **Immediately change the password.**
  - **Protect and not share or publicly post my password. If my password has been compromised, I will report the issue to my supervisor or security personnel.**
  - **Not store my password on any processor, microcomputer, personal digital assistant (PDA), personal electronic device (PED) or other media unless approved by security personnel.**
  - **Be responsible for all activity that occurs on my individual account once my password has been used to log on. If I am a member of a group account, I am responsible for all activity when logged on a system with that account.**
  - **Ensure my password is changed regularly or if compromised.**
  - **Ensure my password meets USDA complexity requirements.**

- **Will use anti-virus software in an effective way to prevent damage or disruption to OCIO operations. I will scan all removable media (e.g., disks, CDs, thumb drives, etc.) for malicious software (e.g., viruses, worms, etc.) before using it on any OCIO computer system or network.**

- **Will take appropriate steps to protect important data from loss (e.g., backups).**

- **Will not use OCIO computers, networks, or IT services for purposes that violate ethical standards, including harassment, threats, sending or accessing sexually explicit material, racially or ethnically demeaning material, gambling, chain letters, for-profit activities, political activities, promotion or solicitation of activities prohibited by law, and so forth. If I use OCIO computer systems and networks for nonofficial purposes, I will do so within the bounds allowed by USDA policy and supervisor approval and without interfering with official business.**

- **Will not try to disable or subvert OCIO security controls or monitoring mechanisms.**

- **Will not attempt to break into any computer, whether Federal, USDA, or private, for which access is not authorized. Attempted break-ins may be authorized by my organization's Information System Security Program Manager (ISSPM) only for functions such as approved security tests, approved attempts to recover a system after a password is lost/forgotten, and similar functions.**

- **Will practice good housekeeping with all electronic equipment, including keeping food, beverages, or other contaminants away from computers and data storage media.**

- **Will report suspected/actual security incidents and other security concerns to my supervisor and my organization's ISSPM.**

- **Will stay abreast of security issues through education and awareness products distributed throughout USDA. I will attend at least one (1) security awareness session each year.**

- **Will not disclose sensitive data. In the course of performing work at OCIO, I realize it may be necessary for me to have access to sensitive information, which includes:**
  - **Proprietary information – technical information or trade secrets, that is proprietary to OCIO.**
  - **Privacy information – information protected under the provisions of the Privacy Act of 1974.**
  - **Privileged information – financial or commercial information that must be restricted from disclosure on the basis of Federal law or contractual agreement.**
  - **Government information – information or data stored, processed or handled in providing services under any OCIO contract.**

_____

(Initials)

OCIO Security Agreement

I have read and understand the OCIO Security Agreement on the use of government Information Technology (IT) systems. I understand that unauthorized or inappropriate use of government IT systems may result in the loss or limitation of my privilege. I also understand that I could face administrative action ranging from counseling to removal from the agency, as well as any criminal penalties or financial liability, depending on the severity of the misuse.

5. EFFECTIVE DATE. This agreement becomes effective when signed and dated. Refusal to sign may result in being denied use of any or all OCIO information systems, including e-mail and network access to the Internet. Refusal to sign does not relieve the individual of responsibility to abide by the standards set forth in this and related documents. (Supervisor/COR/COTR: If the worker refuses to sign, notate that fact on the signature line and retain this document.)

Signature: _____ **Date:** _____

Federal Employee: ☐ **Contractor:** ☐ **(check one)**

Organization: _____

If Contractor – Company Employed By: _____

Supervisor/ COR/COTR Signature: _____ **Date:** _____

Supervisor/ COR/COTR Title: _____